TELKOMNIKA, Vol.17, No.6, December 2019, pp.2912~2918
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v17i6.13285

Study on the performance indicators for smart grids: a comprehensive review

Surender Reddy Salkuti
Deparment of Railroad and Electrical Engineering, Woosong University,
17-2, Woosong University, Jayang-dong, Dong-gu, Daejeon-34606, Republic of Korea
Corresponding author, e-mail: surender.wsu@gmail.com

Abstract

This paper presents a detailed review on performance indicators for smart grid (SG) such as voltage stability enhancement, reliability evaluation, vulnerability assessment, Supervisory Control and Data Acquisition (SCADA) and communication systems. Smart grids reliability assessment can be performed by analytically or by simulation. Analytical method utilizes the load point assessment techniques, whereas the simulation technique uses the Monte Carlo simulation (MCS) technique. The reliability index evaluations will consider the presence or absence of energy storage elements using the simulation technologies such as MCS, and the analytical methods such as systems average interruption frequency index (SAIFI), and other load point indices. This paper also presents the difference between SCADA and substation automation, and the fact that substation automation, though it uses the basic concepts of SCADA, is far more advanced in nature.

Keywords: *communication systems, reliability, smart grid, voltage stability, vulnerability*

1. Introduction

Smart grids (SGs) with renewable energy resources (RERs) provide an effective and alternative solution for the rapidly growing power demand throughout the world. The US energy roadmap study ranks solar photovoltaics (PV), biomass, windmills, and tidal power as the future sources of renewable energy to sustain the economy of the country. Traditional studies on RERs integration have focused on power quality improvement using the RERs, and on their impacts on grid performance [1]. The components that made up the integrated RERs would be wind and solar energy systems, energy storage, load control, and advanced power electronics, which interface between the RERs and the grid provider. Demand response serves as a virtual spinning reserve (SR) to handle the impact of intermittent nature of RERs on the system reliability. Due to the advent of new communication devices and real time applications researchers are diverted to real time approach for vulnerability assessment. Various optimization techniques such as artificial intelligence (AI), expert system or evolutionary programming can be used for the real time applications. To avoid bulk of calculations and for vulnerability indices, the AI techniques are used in recent years as they have various benefits of speedy convergence and improved accuracy of pattern recognition.

A smart grid (SG) architecture showing a SG consisting of the main grid and multiple embedded micro-grids (MGs) is proposed in [2], while [3] proposes an approach to integrate performance indicators of electricity generation plants. The optimization approaches at the base of SGs operation considered the renewable energy share, primary energy consumption, global and local emissions. Various security challenges and threats are reviewed in [4] with respect to their possible sources of occurrence. A multi-objective based robust fuzzy stochastic programming methodology is proposed in [1] to optimize economic, environmental and social costs of network under various uncertain scenarios and parameters. A methodology to investigate the impact of demand response (DR) in a power system with wind energy sources from the perspective of generation adequacy is proposed in [5]. The aim of [6] is to anticipate social acceptance issues related to the deployment of SG by identifying underlying value conflicts. Identified threats to smart grids deployment are classified and presented in [7] based on the technical and non-technical sources of threats. The performance analysis of smart metering for SG enable the researchers, stakeholders, and public policy makers to open

Received June 9, 2019; Revised July 2, 2019; Accepted July 18, 2019

the mind to explore possible in an evolving energy domain as well as beyond this area is presented in [8]. A study to address all standards that define the cyber security requirements applicable to SGs is presented in [9].

This paper presents a detailed review on performance indicators for smart grid (SG) such as voltage stability enhancement, reliability evaluation, vulnerability assessment, Supervisory Control and Data Acquisition (SCADA) and communication systems. It also presents the difference between SCADA and substation automation, and the fact that substation automation, though it uses the basic concepts of SCADA, is far more advanced in nature. The remainder of this paper is organized as follows: section 2 presents the description of voltage stability enhancement. Section 3 presents the evaluation of reliability. Vulnerability assessment is described in section 4. The description of SCADA systems is presented in section 5. The description of communication systems is presented in section 6. The description of demand side management is presented in section 7. Section 8 summarizes the contributions with concluding remarks.

2. Voltage Stability Enhancement

This section reviews the methods to quantify the value added by RERs at distribution levels as it relates to utilities, customers and in the interest of overall national energy security. Measurements matrices are the reliability improvement, cost minimization and voltage stability improvement. There are two levels of voltage stability enhancement in the literature. The first level is with the device-based control, and the second level is in the form of operation-based control. The voltage stability is improved by optimal system operation condition. The static analysis method is used for the determination of preventive control scheme.

As with voltage stability, the characteristics listed below are inherent in the analytic tools for SG. However, it is not included in the analytic tools for the existing electrical power system network. These qualities include scalability, robustness, predictivity, adaptability, stochasticity, and on-line real time data acquisition. Traditional electrical grid is based on large, centralized power station [10]. They supply the grid with RERs through long transmission and distribution system. This architecture has performed very well thorough design for achieving security, reliability and stability. But, with small changes in time, new renewable resources are relatively the system of today. They challenge the users and restore the system. Energy will be guided in distribution from wind, solar with a standalone or grid connected. In this case, whether it is distributed or centrally generated, the standard requirements for a single distribution supply which will meet demand of all kinds and just in time approach requires the need for smart grid. The integration of RERs, Flexible Alternating Current Transmission System (FACTS), Wide Area Management Systems (WAMS), High voltage direct current (HVDC) transmission systems to achieve better stability is introduced in today's grid that has the capability to connect to FACTS cover a number of technologies to overall FACTS devices in smart grid which will facilitate integration of RERs, minimize the risk of overload, to improve dynamic stability, power quality and control load flow studies [11].

Monitoring and control of power system in wide area using the wide area monitoring system has provided the users with full understanding of SG performance in real time [11]. Because of the multiple of data contributing to the states of system in the presence of an electronic device located on the grid is utilized. To achieve this, the control elevation using RERs, HVDC systems, FACTS, WAMS and distribution and/or transmission management system are necessary for the design. WAMS and its associated sensors in the SG environment will allow the real time evaluation of system under various loading and unknown contingencies. Recent advancements in the stability studies aims to address the impacts of contingency, increased nonlinearity of problem space, model and parameter uncertainty and the utilization of available real time data for the enhancement of study is approximated for the management of instability [12].

3. Reliability Evaluation

Smart grids reliability assessment can be performed by analytically or by simulation. Analytical method utilizes the load point assessment techniques, whereas the simulation technique uses the Monte Carlo simulation (MCS) technique [13]. The reliability index

evaluations will consider the presence or absence of energy storage elements using the simulation technologies (i.e., MCS), the analytical methods such as systems average interruption frequency index (SAIFI), and other load point indices. And also, the load flow analysis and other parameter check are done by using the online available data and control using fuzzy controller. Various network configurations will be considered. A number of indices can be computed for the load point assessment [14]. Some of these indices are presented next:

3.1. System Average Interruption Duration Index (SAIDI)

SAIDI is calculated by dividing the sum of total customer interruption durations per year ($\sum U_i N_i$) to total number of customers ($\sum N_i$). This index is expressed by using:

$$SAIDI = \frac{\sum U_i N_i}{\sum N_i} \quad (1)$$

where U_i is outage duration, N_i is total number of customers.

3.2. Customer Average Interruption Duration Index (CAIDI)

CAIDI is calculated by dividing the sum of total customer interruption durations per year ($\sum U_i N_i$) to total number of customers affected ($\sum \lambda_i N_i$). This index is expressed by using:

$$CAIDI = \frac{\sum U_i N_i}{\sum \lambda_i N_i} \quad (2)$$

where λ_i is failure rate.

3.3. Expected Energy Not Served (EENS)

An optimization problem for planning and/or operational purposes using RERs with integrated energy storage technologies has to be considered for the development of SG. The objective of an optimization problem is to minimize EENS or Expected Unserved Energy (EUE), and cost minimization, subjected to various constraints such as the capacity of RERs, network capacity, voltage margin, storage, and reliability margin [15]. EENS is sum of each load (L_i) times its outage duration (U_i). Mathematically, it can be expressed as [16]:

$$EENS = \sum L_i U_i \quad (3)$$

Typical distribution networks will be chosen for both the grid tied and stand-alone power system network. A special distribution load flow program will be utilized to analyze the network under different operating scenarios. The reliability of these systems will be computed based on the variability of RERs. The load flow study and reliability will be recomputed in the presence of energy storage systems (ESSs) and MCS techniques [17].

4. Vulnerability Assessment

Vulnerability assessment is used to determine, identify and rank the contingencies of the system. Power system is a very complex and vulnerable system. Vulnerability assessment in power system provides information on state of system which indicates the system's inability to be stable in any abnormal condition or an unforeseen catastrophic contingency. Vulnerability index is used to determine the strengths and weaknesses of the system against undesired events. There is a list of contingencies that may lead the power system to major blackouts and cascaded failures. Moreover, operating conditions are different according to the location and the system. Vulnerability assessment is a slow process, therefore the real time assessment is very difficult. In a new power system environment, there are lots of measurements are taken, and the verification of these measurements and the development of correlation with vulnerability assessment is quite complex. Evaluation of specific and accurate border line for vulnerability is also a difficult process [18].

There are different approaches used by various researchers for vulnerability assessment. In time domain approach, stability is determined through simulating the generator

behavior. However, it is quite time-consuming process as it involves plenty of nonlinear and differential equations. We can also use a direct method approach using the energy functions. Stability of the system can be determined by comparing the energy value of the system with the critical energy value. This method is being widely used by utilities and researchers as it has a very high speed of convergence [19].

A new method of vulnerability border tracking is by using Partical Swarm Optimization (PSO) along with the Artificial Neural Networks (ANNs). ANN is used for the purpose of increasing the speed of convergence of PSO. PSO is used for better search technique, therefore, it has the benefits of both the systems through one single algorithm. This method is useful for the real time evaluation of vulnerability border. Similarly, many methods can be used together for different applications and combine them to get best optimization results. One such method is to use ANN for vulnerability assessment as it has very good speed of convergence and Fuzzy logic for vulnerability control applications. Fuzzy logic can also be used for locating short circuit faults, which is used for vulnerability contours. This method is useful both for online and offline applications [20]. Fault resistance is also taken into account. Fuzzy logic reasoning is applied to cope with the inherent uncertainty in the problem. The above methods can also be used as a combination of one or more methods and one can develop a hybrid method for vulnerability assessment. Moreover, adaptive dynamic programming (ADP) is also a new approach for vulnerability assessment.

Vulnerability assessment using phasor measurement unit (PMU) is also a new approach. PMUs are used to provide time synchronized data in the form of signals which can later be converted into data (voltage, angle) using various softwares, which contain dynamic information for voltages and angels, and even precursor signals for system collapse. A scheme can be developed to warn the system operator about severe conditions, vulnerabilities and to predict cascading failures using a pattern recognition and phase-space visualization using dynamic data received from PMU [21].

Nowadays, a situational awareness tool based on google maps is used for the advanced power system. It gives the latest system topology and helps the system operator to understand operational conditions not only his own region but also of the neighboring regions to avoid major blackouts [22]. This kind of visualization includes line descriptions, power flows and the status of outage lines, transportation and infrastructure impacts, geo-spatiotemporal information and impacts-population, weather impacts and analysis and predictions results. Moreover, the related data can be overloaded on the system topology. Hence, for various analyses, respective data is readily available. Two types of vulnerability indexes namely power system loss (PSL) and anticipated loss of load (ALL) are used for different contingences. Application of Geographical Information System (GIS) also helps in developing the vulnerability assessment [23].

5. SCADA Systems

Supervisory Control and Data Acquisition (SCADA) pertains to automation and the concepts of automation borrow from SCADA. Before it gets into the SCADA part, it presents the important terminologies and components of SCADA which are used in the substation automation [24]. The functions of each of the components are presented next:

Remote Terminal Unit (RTU): It processes the data input (both analog and digital), and converts it into digital output which can either be seen on a single screen Human Machine Interface (HMI) in the control room itself or it can be transmitted over the Ethernet to other places for remote control. The function of Front-End Processors (FEP) is to act as an interface between the computer system, and the RTUs located locally and at remote substations. There are two FEPs at each site, both functional simultaneously, and also any one FEP capable of fully taking over the functions of the other FEP. Each FEP has a dual LAN interface and houses multiple Remote Channel Controller (RCC) modules, according to the number of RTUs connected to the control center. These RCC modules provide RS-232 interface ports for connecting to the RTUs [25]. The RCC modules are of microprocessor-based design and are able to:

- operate independently and support a different RTU protocol on individual channels
- utilize drivers to establish the RTU communications

- conduct simultaneous RTU communications on each channel, acquire data, perform message security checks, and decode the data
- process the data.
- buffer all data for transfer to the controlling server.

The FEP transfers data to the controlling server in a timely fashion. The FEP also responds to the controlling server's demands for performing the required functions at the RTUs. The RCC channel capacity covers the entire complement of RTUs which consists of the new RTUs and the existing RTUs. The channels are expandable in the future to ultimate quantity by acquiring and inserting RCC modules. All critical RTUs are provided with 2 communication channels right from the control center up to the RTU, and these channels are connected one on each FEP. The Remote Communication Controller (RCC) interfaces with the FEP through the VME bus. Redundant FEPs and RCCs are provided with automatic changeover from one to the other when any FEP or RCC fails. When a modem fails or a communication link to a critical RTU goes down, there is automatic changeover from the defective link/modem to an alternate link/modem. All critical RTUs are provided with redundant communication channels [26].

Critical RTUs have the capability to switch between redundant communication channels when the system detects a communication channel failure. To satisfy the redundancy requirements, each communication channel is switched between a primary and backup port under failure conditions. In the GE Harris Energy Control Systems implementation, redundancy is provided all the way up to the remote RTU communication interface, using redundant FEPs, RCCs and separate channels to connect to the RTU. Any single failure is protected against by this method [27].

a. Human Machine Interface (HMI): The HMI/SCADA industry was essentially born out of a requirement for a user friendly front-end to control system containing programmable logic controllers (PLC).
b. Central Control Room Computer: Usually, the HMI/SCADA presents the information in the form of a mimic, which means that the operator can see a representation of the plant being controlled.
c. Transducers: They are the energy converters which convert one from of energy to another. It is used in substations to convert the measured AC voltages and currents (measured from the CT and CVT inputs) and convert them into a common DC current. They can be self-powered or separately powered. In self powered transducers, the components of the transducer are powered by the source itself, where as in separately powered transducers, there is an external source which is used to run the circuit of the transducer.
d. Multiplexer: It is a device that can interleave two or more activities. For example, a 16:1 multiplexer can take 16 different inputs and can create a time sharing mechanism that will allow it to give the required output of the 16 inputs based on a predefined logic. The simplest logic generally used is a clock pulse. Though automation basically involves all the concepts of SCADA and though they are terms that are used interchangeably, there exist certain basic differences between them [28], and they are listed below:
    - Conventional SCADA deals with data acquisition and control of most of the equipment in the substation, but it cannot be used for relays for the basic reason that they have to be manually operated. Whereas, the substation automation involves automation of relays and including them in the data acquisition and control process. The numerical relays used in substation automation systems act as a virtual RTU. In other words, the SCADA system applied to protection can be referred to as substation automation systems.
    - SCADA uses the concept of transducers, which are electronic devices that invariably cause a lag or delay in the transmission of data, whereas substation automation system aims at minimizing the data transmission time by removing the use of transducers.
    - Substation automation system needs to have higher accuracy than the conventional SCADA system as it involves the protection of switchgear of a substation. Thus, it removes the transducers, which approximate the values, and the obtained values directly from the devices.
    - Conventional SCADA has the concept of a single RTU, where the data is acquired and stored. The required control is performed form the centralized RTU itself. In such a case, a malfunction even in a part of the RTU affects the whole system. Whereas, in a substation automation system, the information and control are decentralized, i.e., each bay acts as a virtual RTU itself and sends the information into the control room.

The control can be performed from any level based on the control hierarchy. Hence, substation automation system can also be referred to as an integrated SCADA system.

6. Communication Systems

Communication infrastructure is very important for successful operation of SGs. The use of communication systems ensures the reduction of optimal operation and energy consumption of SG and the coordination between all its components from generation to the end users. There are several existing communication technologies available for the implementation in SGs include Power Line Carrier Communication (PLCC), WLAN, ZigBee, WiMAX, cellular communication [29]. Smart metering communication system consists a smart meter which is a two-way communicating equipment that measures the energy consuming at the appliances such as gas, electricity, water or heat, etc. Smart metering communication system also consists of Home Area Network (HAN), Neighborhood Area Network (NAN) and Wide Area Network (WAN) [30]. HAN is an information and communication network formed by appliances and devices within a home to support different distributed applications. NAN collects the data from multiple HANs and delivers the data to a data concentrator. WAN is the data transport network that carries metering data to central control centers [31].

Power Line Carrier Communication (PLCC) is one of the common communication systems. Using the EHV transmission line as a medium, the link is established among the stations connected with the transmission network [29]. It is used to serve voice communication, data transmission, and transmission of carrier-aided trip signal for the reduction of tripping time for the remote circuit breaker or in other words, reduction of fault feeding time during occurrence of fault in the transmission line. Basic equipments for PLCC are outdoor and indoor equipments. The outdoor equipments include line trap, capacitive voltage transformers (CVT)/coupling capacitors (CC), line matching unit with protective device, and co-axial cable. Indoor equipments include power line carrier set, dialing exchange and phone sets, RTU, interface cubicle and modem, and protection coupler [32]. It is important to mention here that the outdoor equipments are connected with the transmission line in different ways known as mode of coupling, and this is very vital for the faithful transmission/reproduction of PLCC signal.

7. Conclusions

This paper presents a detailed review on performance indicators for smart grid (SG) such as voltage stability enhancement, reliability evaluation, vulnerability assessment, SCADA and communication systems. Communication infrastructure is very important for successful operation of smart grids, and the use of it ensures the reduction of optimal operation and energy consumption of SG and the coordination between all its components from generation to the end users. Vulnerability assessment is used to determine, identify and rank the contingencies of the system. Vulnerability index is used to determine the strengths and weaknesses of the system against undesired events. There is a list of contingencies that may lead the power system to major blackouts and cascaded failures.

Acknowledgements

This research work has been carried out based on the support of “Woosong University's Academic Research Funding-2019”.

References

[1] Tsao YC, Thanh VV, Lu JC. Multiobjective robust fuzzy stochastic approach for sustainable smart grid design. *Energy*. 2019; 176: 929-939.
[2] Worighi I, Maac A, Hafid A, Hegazy O, Mierlo JV. Integrating renewable energy in smart grid system: Architecture, virtualization and analysis. *Sustainable Energy, Grids and Networks*. 2019; 18: 100226.
[3] Noussan M. Performance based approach for electricity generation in smart grids. *Applied Energy*. 2018; 220: 231-241.
[4] OkinoOtuoze A, Mustafa MW, Larik RM. Smart grids security challenges: Classification by sources of threats. *Journal of Electrical Systems and Information Technology*. 2018; 5(3): 468-483.

[5] Gao J, Ma Z, Guo F. The influence of demand response on wind-integrated power system considering participation of the demand side. *Energy*. 2019; 178: 723-738.
[6] Wildt TED, Chappin EJL, Kaa GVD, Herder PM, Poel IRVD. Conflicting values in the smart electricity grid a comprehensive overview. *Renewable and Sustainable Energy Review*s. 2019; 111: 184-196.
[7] Otuoze AO, Mustafa MW, Larik RM. Smart grids security challenges: Classification by sources of threats. *Journal of Electrical Systems and Information Technology*. 2018; 5(3): 468-483.
[8] Sharma K, Saini LM. Performance analysis of smart metering for smart grid: An overview. *Renewable and Sustainable Energy Reviews*. 2015; 49: 720-735.
[9] Leszczyna R. A review of standards with cybersecurity requirements for smart grid. *Computers & Security*. 2018; 77: 262-276.
[10] Momoh JA. Adaptive Stochastic Optimization Techniques with Applications. CRC Press. 2015.
[11] Ahmed S, Khaliq A, Noman ud Din S, Ud Din S. *Stability enhancement in smart grid by using superconducting fault current limiter*. Symposium on Recent Advances in Electrical Engineering (RAEE). Islamabad. 2015: 1-7.
[12] Hridya KR, Mini V, Visakhan R, Kurian AA. *Analysis of voltage stability enhancement of a grid and loss reduction using series FACTS controllers*. International Conference on Power, Instrumentation, Control and Computing (PICC). Thrissur. 2015:1-5.
[13] Kulkarni N, Lalitha SVNL, Deokar SA. Real time control and monitoring of grid power systems using cloud computing. *International Journal of Electrical and Computer Engineering*. 2019; 9(2): 941-949.
[14] Li J, Li T, Han L. Research on the Evaluation Model of a Smart Grid Development Level Based on Differentiation of Development Demand. *Sustainability*. 2018; 10: 1-25.
[15] Lee J, Kim SB, Park GL. Data Analysis for Solar Energy Generation in a University Microgrid. *International Journal of Electrical and Computer Engineering*. 2018; 8(3): 1324-1330.
[16] Refaat SS, Abu-Rub H, Trabelsi M, Mohamed A. *Reliability evaluation of smart grid system with large penetration of distributed energy resources*. IEEE International Conference on Industrial Technology (ICIT). Lyon. 2018: 1279-1284.
[17] Qasaimeh M, Turab R, Al-Qassas RS. Authentication techniques in smart grid: a systematic review. *TELKOMNIKA Telecommunication Computing Electronics and Control*. 2019; 17(3): 1584-1594.
[18] Parate M, Tajane S, Indi B. *Assessment of System Vulnerability for Smart Grid Applications.* IEEE International Conference on Engineering and Technology (ICETECH). Coimbatore. 2016: 1083-1088.
[19] Leszczyna R. Standards on cyber security assessment of smart grid. *International Journal of Critical Infrastructure Protection*. 2018; 22: 70-89.
[20] Jung CM, Ray P, Salkuti SR. Asset management and maintenance: a smart grid perspective. *International Journal of Electrical and Computer Engineering*. 2019; 9(5): 3391-3398.
[21] Che Y, Jia J, Zhao Y, He D, Cao T. Vulnerability assessment of urban power grid based on combination evaluation. *Safety Science*. 2019; 113: 144-153.
[22] Shen Y, Gu C, Zhao P. Structural Vulnerability Assessment of Multi-energy System Using a PageRank Algorithm. *Energy Procedia*. 2019; 158: 6466-6471.
[23] Peterson J, Haney M, Borrelli RA. An overview of methodologies for cybersecurity vulnerability assessments conducted in nuclear power plants. *Nuclear Engineering and Design*. 2019; 346: 75-84.
[24] Sallam AA, Malik OP. Scada Systems and Smart Grid Vision. *Electric Distribution Systems*. 2011: 469-493.
[25] Sayed K, Gabbar HA. SCADA and smart energy grid control automation. In: Gabbar HA. *Editor*. Smart Energy Grid Engineering. Academic Press*.* 2017: 481-514.
[26] Nguyen VH, Tran QT, Besanger Y. SCADA as a service approach for interoperability of micro-grid platforms. *Sustainable Energy, Grids and Networks*. 2016; 8: 26-36.
[27] Arafa MIA, Said ESSA. A different vision for uninterruptible load using hybrid solar-grid energy. *International Journal of Power Electronics and Drive System*. 2019; 10(1): 381-387.
[28] Knapp ED, Samani R. Chapter 5 - Security Models for SCADA, ICS, and Smart Grid Applied Cyber Security and the Smart Grid, Implementing Security Controls into the Modern Power Infrastructure. 2013: 101-123.
[29] Baimel D, Tapuchi S, Baimel N. *Smart grid communication technologies- overview, research challenges and opportunities*. International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM). Anacapri. 2016: 116-120.
[30] Fan Z. Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities. *IEEE Communications Surveys & Tutorials*. 2013; 15(1): 21-38.
[31] Emmanuel M, Rayudu R. Communication technologies for smart grid applications: A survey. *Journal of Network and Computer Applications*. 2016; 74: 133-148.
[32] Nadour M, Essadki A, Nasser T, Fdaili M. Robust coordinated control using backstepping of flywheel energy storage system and DFIG for power smoothing in wind power plants. *International Journal of Power Electronics and Drive System*. 2019; 10(2): 1110-1122.